STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: User Responsibility

Product ID: ENT-SEC-081

Effective Date: August 2, 2001

Approved: BARBARA RANF, Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all state employees and state contractors using a state computer. This policy does not apply to students/employees of the Montana University Systems who are employed by the System and are not full time employees.

B. Requirements

Each user of the State of Montana's computing and information resources should realize the fundamental importance of information resources and is responsible for the safe keeping of these resources.

Users and system administrators must guard against abuses that disrupt or threaten the viability of all systems, including those on the State network and those on networks to which State systems are connected.

Each user is responsible for having knowledge of the State's policies concerning security and care for their computer. It is the responsibility of the State to educate its management and staff about these policies; to educate its employees about the dangers of computer abuse and its threat to the operation of the State computer network; and educate its management and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues.

Each user of the State of Montana's computing and information resources must act responsibly. Each user is responsible for the integrity of these resources. All users of State-owned or State-leased computing systems must be knowledgeable of and adhere to agency policies, respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource, respect the integrity of the physical facilities and controls, and obey all federal, state, county, and local laws and ordinances. All employees must abide by these policies, relevant laws and contractual obligations, and appropriate ethical standards.

State computing facilities and UserIDs are to be used for the job-related activities for which they are assigned. State computing resources are not to be used for the following:

- private commercial purposes,
- non-State-related activities (including games or software that is not required for an employees job responsibilities), or
- non-State standard software. Exceptions can be granted by ITSD for the use of software for which a State standard exists.

1. Consent Form

All State employees or contractors with the state who have access to the Internet, email, or other online services, will sign a consent form indicating that they have knowledge of the state's policies and procedures in regards to the use of state computing resources. Privacy in using the state's computer systems is not guaranteed. Therefore, employees should not have any expectations of privacy when using the Internet, email, or other computer services. The following is an example consent form that agencies can use for employees and contractors.

2. Sample Consent Form

I _____ have read the State of Montana's computer use policies and agree to comply with all terms and conditions. I agree that all network activity conducted while doing State business and being conducted with State resources is the property of the State of Montana.

I understand that the State reserves the right to monitor and log all network activity including email and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

Signed_____

Date_____

3. Misuse Of Computer Resources

The following items represent, but do not fully define, misuse of computing and information resources:

Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.

Down-loading, installing, or running security programs or utilities which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.

Use of computers and userIDs for which there is no authorization, or use of userIDs for purpose(s) outside of those for which they have been issued.

Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non, -work related software on State-owned equipment.

Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the State. (That

is, if you abuse the networks to which the State has access or the computers at other sites connected to those networks, the State will treat this matter as an abuse of your computing privileges.)

Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.

The use of computing facilities, UserIDs, or computer data for purposes other than those for which they were intended or authorized.

Sending fraudulent email, breaking into another user's emailbox, or unauthorized personnel reading someone else's email without his or her permission.

Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.

Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

Taking advantage of another user's naiveté or negligence to gain access to any UserID, data, software, or file that is not your own and for which you have not received explicit authorization to access.

Physically interfering with other users' access to the State's computing facilities.

Encroaching on or disrupting others' use of the State's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a State computer; damaging or vandalizing State computing facilities, equipment, software, or computer files).

Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.

Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.

Knowingly transferring or allowing to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.

4. Reporting And Disciplinary Action

Users will cooperate with system administrator requests for information about computing activities; follow agency procedures and guidelines in handling

diskettes and external files in order to maintain a secure, virus-free computing environment; follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location; and honor the Acceptable Use Policies of any non-State networks accessed.

Users will report unacceptable use and other security violations to their immediate supervisor, to local personnel responsible for local network policy enforcement, or to personnel responsible for the security and enforcement of network policies where the violation originated.

Misuse of the state's computer resources may result in an agency taking disciplinary action appropriate to the misuse, up to and including termination.

C. Background - History On The Creation Of Or Changes To This Policy

This policy was originally created by the NetWare Managers Group Policy Committee.

D. Guidelines - Recommendations, Not Requirements

All entities that use the state's network that are not included within the scope of this policy are encouraged to adopt a similar policy.

E. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- 2-17-503, MCA;
- 2-15-114, MCA;
- 45-6-311, MCA;
- 2-2-121, MCA;

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- MOM 1-0250.00 - 1-0250.00, MOM;
- Internet Services Policy
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-081
Proponent:	BARBARA RANF, Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	August 2, 2001
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.